



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/689,157	10/20/2003	Andrew M. Spencer	10013891-1	9457

22879 7590 11/27/2009
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER

TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
----------	--------------

2438

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

11/27/2009

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

Office Action Summary	Application No. 10/689,157	Applicant(s) SPENCER, ANDREW M.	
	Examiner THANHNGA B. TRUONG	Art Unit 2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 July 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26, 28 and 29 is/are pending in the application.
- 4a) Of the above claim(s) 16-26 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-15 and 28-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is responsive to the communication filed on July 29, 2009. Claims 1-26 and 28-29 are pending. Claims 16-26 are withdrawn and claims 27 and 30 are cancelled by the applicant. At this time, claims 1-15 and 28-29 are still rejected.

In preparing for this office action, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Response to Arguments

2. Applicant's arguments filed July 29, 2009 under claim objection have been fully considered and are persuasive.

Applicant's arguments filed July 29, 2009 under 35 USC 102 and under 35 USC 102 or, in the alternative, under 35 U.S.C. 103(a) have been fully considered but they are not persuasive.

Applicant argues that:

While Eisele discloses loading cryptographic algorithms into the diskette memory in a way that they cannot be reproduced and the use of such cryptographic algorithms to encrypt data received at a diskette, Eisele does not disclose the use of a non-volatile memory configured to store a master encryption key and the use of a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key as recited by claims 1-15. There is no teaching in Eisele directed to the use of a master encryption key to encrypt encryption

Art Unit: 2438

keys. Furthermore, Eisele does not teach the use of two different memories to store encryption keys, i.e. a non-volatile memory to store the master encryption key and a non-volatile magnetic memory to store the encrypted encryption keys as recited by claims 1-15.

Examiner respectfully disagrees and still maintains that:

Eisele does teach the claimed subject matter. It is clearly in Figure 2, 3, and 8, element 9 is a memory and column 5, lines 20-24 of Eisele stated that in order to use any of the elements as an encryption/decryption machine, it is necessary to load the element's memory units with one or more cryptographic algorithms, secret codes etc. (e.g., encryption key or master encryption key, etc..) in such a way that they cannot be reproduced. Figure 3 of Eisele clearly discloses element 9 is non-volatile memory and disk 7 is non-volatile magnetic memory. Therefore, Eisele precisely teaches the use of the two different memories to store encryption keys, i.e. a non-volatile memory to store the master encryption key and a non-volatile magnetic memory to store the encrypted encryption keys as recited by claims 1-15.

Applicant further argues that:

While Eisele discloses the use of a diskette processor 2 to encrypt and decrypt data, Eisele does not disclose reading encrypted encryption keys from a magnetic random access memory, reading a master encryption key from a first non-volatile memory and decrypting each one of the encryption keys using the master encryption key. There is no teaching in Eisele directed to the use of a master encryption key to decrypt encrypted encryption keys. Furthermore, Eisele does not disclose the use of two different memories, i.e. reading encrypted encryption keys from a magnetic random access memory and reading a master encryption key from a first non-volatile memory as recited by claims 28-29. Since Eisele fails to disclose each and every element recited by claims 28-29, Applicant respectfully requests the withdrawal of the rejection of such claims as being anticipated by Eisele.

Examiner respectfully disagrees and still maintains that:

Eisele does teach the claimed subject matter. As a matter of fact, in order to verify user-authorization a PIN-code is necessary which is entered either on the keyboard of the EDP-equipment and communicated through the relevant interface (6, 8, 26) into processor 2 or, if the element itself is equipped with a key pad, entered into its key pad. At this point, the PIN is verified, the result of which procedure is passed back to the EDP-equipment via the interface. The alteration of the PIN-code or similar information kept in processor 2 or its memory 9 is also possible (assuming the necessary authorization) using a similar procedure. It is also possible to use the invented device to check whether the user is working on the correct computer. Accordingly the central computer asks the user for an additional secret code after the PIN has been verified which is also verified by processor 2. The result of this procedure can be shown on display 22 (column 4, line 60 through column 5, line 8 of Eisele). It is common standard and obvious that when secret code, PIN, encryption key, or master encryption key needed to verify, one must understand that these secret code, PIN, encryption key, or master encryption key must be read out or retrieve from the memory to compare for the matching code before authorizing the user to access. Furthermore, Eisele also discloses it is of particular advantage also to be able to use processor 2 in the various elements to **encrypt and decrypt data** (emphasis added) by transmitting plaintext data to processor 2 through the interface and back in encrypted form through this interface (column 5, lines 12-16 of Eisele). Figure 3 of Eisele clearly discloses element 9 is non-volatile memory and disk 7 is non-volatile magnetic memory. Therefore, Eisele precisely teaches the use of the two different memories to store encryption keys, i.e. reading encrypted encryption keys from a magnetic random access memory and reading a master encryption key from a first non-volatile memory as recited by claims 28-29.

The fact that Examiner may not have specifically responded to any particular arguments made by Applicant and Applicant's Representative should not be construed as indicating Examiner's agreement therewith.

For the above reasons, it is believed that the rejections should be sustained.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Eisele (US 5,159,182).

a. Referring to claim 1:

i. Eisele teaches a removable information storage device (see Figures 2 and 3) suitable for use with a host, comprising:

(1) a non-volatile memory (e.g. memory 9) configured to store a master encryption key (**see Figures 2, 3, and 8, element 9; column 4, lines 6 and 40; and column 5, lines 20-24 of Eisele**); and

(2) a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys (**see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele**).

6. Claims 2-15, 28-29 are rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Eisele (US 5,159,182).

a. Referring to claim 28:

i. Eisele teaches a method of encrypting encryption keys using a master encryption key in an information storage device, comprising:

(1) reading encrypted encryption keys from a magnetic random access memory; reading a master encryption key from a non-volatile memory (**see Figures 5-6; and column 5, lines 5-9 of Eisele**);

(2) decrypting each one of the encryption keys using the master encryption key **(column 5, lines 12-19 of Eisele)**;

(3) encrypting data using the encryption keys **(column 5, lines 12-19 of Eisele)**; and

(4) writing (e. g., storing) the encrypted data to the magnetic random access memory **(see Figures 2-3 and column 5, lines 12-24 of Eisele)**.

ii. Although Eisele teaches the claimed subject matter, Eisele does not clearly use the term “magnetic random access memory (MRAM)” for disk 7 as shown in Figure 3. However, Eisele implies that the magnetic disk includes read/write heads 16 and 17, wherein MRAM uses the same read/write functionality as in disk 7 of Eisele.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Eisele to clearly disclose disk 7 as being a magnetic random access memory (MRAM) **(see Figure 3)**.

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Eisele to clearly name the removable storage device disk 7 as any different type of programmable memory or storage device to store encryption keys, master keys, encryption/decryption data, program, etc.

b. Referring to claim 29:

i. Eisele further teaches:

(1) reading encrypted data from the magnetic random access memory **(see Figures 5-6; and column 5, lines 5-9 of Eisele)**; and

(2) decrypting the encrypted data using the encryption keys **(column 5, lines 12-19 of Eisele)**.

c. Referring to claim 2:

i. Eisele further teaches:

(1) an encryption and decryption engine configured to encrypt and decrypt the encryption keys using the master encryption key and to encrypt and decrypt the data using one or more of the encryption keys (**column 5, lines 12-19 of Eisele**).

d. Referring to claim 3:

i. Eisele further teaches:

(1) wherein the first non-volatile memory is a magnetic memory (**see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele**).

e. Referring to claim 4:

i. Eisele further teaches:

(1) wherein the first non-volatile memory is a read-only memory which includes fuse elements (**see Figures 2, 3, and 8, element 9; column 4, lines 6 and 40; and column 5, lines 20-24 of Eisele**).

f. Referring to claim 5:

i. Eisele further teaches:

(1) wherein the first non-volatile memory is a nitrided read-only memory (**see Figures 2, 3, and 8, element 9; column 4, lines 6 and 40; and column 5, lines 20-24 of Eisele**).

g. Referring to claim 6:

i. Eisele further teaches:

(1) wherein the first non-volatile memory is an erasable programmable read-only memory (**see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele**).

h. Referring to claim 7:

i. Eisele further teaches:

(1) wherein the first non-volatile memory is an electronically erasable programmable read-only memory (**see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele**).

Art Unit: 2438

i. Referring to claim 8:

i. Eisele further teaches:

(1) wherein the first non-volatile memory is a flash erasable programmable read-only memory (**see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele**).

k. Referring to claim 9:

i. Eisele further teaches:

(1) wherein the first non-volatile memory is a one time programmable read-only memory (**see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele**).

l. Referring to claim 10:

i. Eisele further teaches:

(1) wherein the non-volatile magnetic memory is a magnetic random access memory (**see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele**).

m. Referring to claim 11:

i. Eisele further teaches:

(1) wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the second areas (**column 5, lines 20-30 of Eisele**).

n. Referring to claims 12-13:

i. These claims have limitations that is similar to those of claim 11, thus they are rejected with the same rationale applied against claim 11 above.

o. Referring to claim 14:

i. Eisele further teaches:

(1) wherein the first areas are located at one or more predetermined address locations within the second non-volatile memory (**column 5, lines 20-30 of Eisele**).

p. Referring to claim 15:

Art Unit: 2438

i. Eisele further teaches:

(1) wherein the first areas are located at one or more random address locations within the second non-volatile memory (**column 5, lines 20-30 of Eisele**).

Conclusion

7. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached at 571-272-3787. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/

Primary Examiner, Art Unit 2438

Application/Control Number: 10/689,157

Page 10

Art Unit: 2438

TBT

November 21, 2009